

The SLOCC invariant and the residual entanglement for n -qubits *

Dafa Li

Dept of mathematical sciences
Tsinghua University, Beijing 100084 CHINA
email address: dli@math.tsinghua.edu.cn

Xiangrong Li

Department of Mathematics
University of California, Irvine, CA 92697-3875, USA

Hongtao Huang

Electrical Engineering and Computer Science Department
University of Michigan, Ann Arbor, MI 48109, USA

Xinxin Li

Dept. of computer science
Wayne State University, Detroit, MI 48202, USA

February 5, 2008

Abstract

In this paper, we find the invariant for n -qubits and propose the residual entanglement for n -qubits by means of the invariant. Thus, we establish a relation between SLOCC entanglement and the residual entanglement. The invariant and the residual entanglement can be used for SLOCC entanglement classification for n -qubits.

PACS numbers: 03.67.-a, 03.65.Ta, 89.70.+c

Keywords: Concurrence, quantum computing, the residual entanglement, SLOCC entanglement classification, SLOCC invariant.

1 Introduction

Entanglement plays a key role in quantum computing and quantum information. If two states can be obtained from each other by means of local operations and classical communication (LOCC) with nonzero probability, we say that two states have the same kind of entanglement[1]. Recently, many authors have studied the equivalence classes of three-qubit states specified SLOCC (stochastic local operations and classical communication) [3]–[15]. Dür et al. showed that for pure states of three-qubits there are six inequivalent entanglement classes[4]. A. Miyake discussed the onionlike classification of SLOCC orbits and proposed the SLOCC equivalence classes using the orbits[10]. A.K. Rajagopal and R.W. Rendell gave the conditions for the full separability and the biseparability[12]. In [13] we gave the simple criteria for the complete SLOCC classification for three-qubits. In [14] we presented the invariant for 4-qubits and used the invariant for SLOCC entanglement classification for 4-qubits. Verstraete et al.[9] considered the entanglement classes

*The paper was supported by NSFC(Grant No. 60433050), the basic research fund of Tsinghua university No: JC2003043 and partially by the state key lab. of intelligence technology and system

of four-qubits under SLOCC and concluded that there exist nine families of states corresponding to nine different ways of entanglement.

Coffman et al. presented the concurrence and the residual entanglement for 2 and 3-qubits[16]. It was proven that the residual entanglement for 3-qubits or 3-tangle is an entanglement monotone[4]. The general residual entanglement was discussed in [17]. Wong and Nelson presented n -tangle for even n -qubits[18]. For odd n -qubits, they did not define n -tangle. Osterloh and Siewert constructed N -qubit entanglement monotone from antilinear operators[19][20].

In this paper, we find the SLOCC invariant for n -qubits and extend Coffman et al. 's residual entanglement or 3-tangle for 3-qubits to n -qubits in terms of the invariant. The necessary D -criteria and F -criteria for SLOCC classification are also given in this paper. Using the invariant, the residual entanglement and the criteria, it can be determined that if two states belong to different SLOCC entanglement classes. The invariant, the residual entanglement and the criteria only require simple arithmetic operations: multiplication, addition and subtraction.

The paper is organized as follows. In section 2, we present the invariant for n -qubits and prove the invariant by induction in Appendix D. In section 3, we propose the residual entanglement for n -qubits and investigate properties of the residual entanglement. In section 4, we exploit SLOCC entanglement classification for n -qubits.

2 The SLOCC invariant for n -qubits

Let $|\psi\rangle$ and $|\psi'\rangle$ be any states of n -qubits. Then we can write

$$|\psi\rangle = \sum_{i=0}^{2^n-1} a_i |i\rangle, |\psi'\rangle = \sum_{i=0}^{2^n-1} b_i |i\rangle,$$

where $\sum_{i=0}^{2^n-1} |a_i|^2 = 1$ and $\sum_{i=0}^{2^n-1} |b_i|^2 = 1$.

Two states $|\psi\rangle$ and $|\psi'\rangle$ are equivalent under SLOCC if and only if there exist invertible local operators $\alpha, \beta, \gamma, \dots$ such that

$$|\psi\rangle = \underbrace{\alpha \otimes \beta \otimes \gamma \cdots}_n |\psi'\rangle, \quad (2.1)$$

where the local operators $\alpha, \beta, \gamma, \dots$, can be expressed as 2×2 invertible matrices as follows.

$$\alpha = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix}, \beta = \begin{pmatrix} \beta_1 & \beta_2 \\ \beta_3 & \beta_4 \end{pmatrix}, \gamma = \begin{pmatrix} \gamma_1 & \gamma_2 \\ \gamma_3 & \gamma_4 \end{pmatrix}, \dots$$

We reported the invariants for 2-qubits, 3-qubits and 4-qubits in [14]. When n is small, by solving the corresponding matrix equations in (2.1), we can obtain the amplitudes a_i . Then, it is easy to verify the invariants for 2-qubits, 3-qubits and 4-qubits. However, when n is large, it is hard to solve the matrix equations in (2.1).

We define function $sign(n, i) = \pm 1$ to describe the invariant below.

Always $sign(2, 0) = sign(3, 0) = 1$. For $n \geq 4$ and $0 \leq i \leq 2^{n-3} - 1$, we define $sign(n, i)$ as follows.

When $0 \leq i \leq 2^{n-4} - 1$, $sign(n, i) = sign(n-1, i)$. When $2^{n-4} - 1 < i \leq 2^{n-3} - 1$, $sign(n, i) = sign(n, 2^{n-3} - 1 - i)$ provided that n is odd; when n is even, $sign(n, i) = -sign(n, 2^{n-3} - 1 - i)$.

2.1 The SLOCC invariant for even n -qubits

2.1.1 For 2-qubits

If $|\psi\rangle$ and $|\psi'\rangle$ are equivalent under SLOCC, then they satisfy the following equation,

$$a_0 a_3 - a_1 a_2 = (b_0 b_3 - b_1 b_2) \det(\alpha) \det(\beta). \quad (2.2)$$

(2.2) guarantees that $(b_0 b_3 - b_1 b_2)$ does not vary when $\det(\alpha) \det(\beta) = 1$ or vanish under SLOCC operators α and β .

2.1.2 For 4-qubits

$|\psi\rangle$ and $|\psi'\rangle$ are equivalent under SLOCC if and only if there exist invertible local operators α , β , γ and δ such that

$$|\psi\rangle = \alpha \otimes \beta \otimes \gamma \otimes \delta |\psi'\rangle, \quad (2.3)$$

where

$$\delta = \begin{pmatrix} \delta_1 & \delta_2 \\ \delta_3 & \delta_4 \end{pmatrix}.$$

Let

$$IV(a, 4) = (a_0 a_{15} - a_1 a_{14}) + (a_6 a_9 - a_7 a_8) - (a_2 a_{13} - a_3 a_{12}) - (a_4 a_{11} - a_5 a_{10})$$

and

$$IV(b, 4) = ((b_0 b_{15} - b_1 b_{14}) + (b_6 b_9 - b_7 b_8) - (b_2 b_{13} - b_3 b_{12}) - (b_4 b_{11} - b_5 b_{10})).$$

Then, if $|\psi\rangle$ and $|\psi'\rangle$ are equivalent under SLOCC, then we have the following equation:

$$IV(a, 4) = IV(b, 4) * \det(\alpha) \det(\beta) \det(\gamma) \det(\delta). \quad (2.4)$$

In Appendix A of this paper, we give a formal derivation of (2.4). The ideas for the proof will be used to by induction derive the following Theorem 1.

By (2.4), $IV(b, 4)$ does not vary when $\det(\alpha) \det(\beta) \det(\gamma) \det(\delta) = 1$ or vanish under SLOCC operators.

2.1.3 The definition and proof of the invariant for even n -qubits

Let $|\psi\rangle$ and $|\psi'\rangle$ be any pure states of n -qubits.

Version 1 of the invariant

When $n \geq 4$, let

$$\begin{aligned} IV(a, n) = & \sum_{i=0}^{2^{n-3}-1} \text{sign}(n, i) [(a_{2i} a_{(2^n-1)-2i} - a_{2i+1} a_{(2^n-2)-2i}) \\ & + (a_{(2^{n-1}-2)-2i} a_{(2^{n-1}+1)+2i} - a_{(2^{n-1}-1)-2i} a_{2^{n-1}+2i})]. \end{aligned} \quad (2.5)$$

Theorem 1.

For $n(\geq 4)$ -qubits, assume that $|\psi\rangle$ and $|\psi'\rangle$ are equivalent under SLOCC. Then the amplitudes of the two states satisfy the following equation,

$$IV(a, n) = IV(b, n) \underbrace{\det(\alpha) \det(\beta) \det(\gamma) \dots}_n, \quad (2.6)$$

where $IV(b, n)$ is obtained from $IV(a, n)$ by replacing a in $IV(a, n)$ by b .

An inductive proof of Theorem 1 is put in Part 1 of Appendix D.

By (2.6), clearly $IV(b, n)$ does not vary when $\det(\alpha) \det(\beta) \det(\gamma) \dots = 1$ or vanish under SLOCC operators. So, here, $IV(b, n)$ is called as an invariant of even n -qubits.

So far, no one has reported the invariant for 6-qubits. Therefore, it is valuable to verify that (2.6) holds when $n = 6$.

For 6-qubits,

$|\psi\rangle$ and $|\psi'\rangle$ are equivalent under SLOCC if and only if there exist invertible local operators α , β , γ , δ , σ and τ such that

$$|\psi\rangle = \alpha \otimes \beta \otimes \gamma \otimes \delta \otimes \sigma \otimes \tau |\psi'\rangle, \quad (2.7)$$

where $\sigma = \begin{pmatrix} \sigma_1 & \sigma_2 \\ \sigma_3 & \sigma_4 \end{pmatrix}$ and $\tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_3 & \tau_4 \end{pmatrix}$.

From (2.5),

$$\begin{aligned} IV(a, 6) = & (a_0a_{63} - a_1a_{62}) + (a_{30}a_{33} - a_{31}a_{32}) - (a_2a_{61} - a_3a_{60}) - (a_{28}a_{35} - a_{29}a_{34}) \\ & - (a_4a_{59} - a_5a_{58}) - (a_{26}a_{37} - a_{27}a_{36}) + (a_6a_{57} - a_7a_{56}) + (a_{24}a_{39} - a_{25}a_{38}) \\ & - (a_8a_{55} - a_9a_{54}) - (a_{22}a_{41} - a_{23}a_{40}) + (a_{10}a_{53} - a_{11}a_{52}) + (a_{20}a_{43} - a_{21}a_{42}) \\ & + (a_{12}a_{51} - a_{13}a_{50}) + (a_{18}a_{45} - a_{19}a_{44}) - (a_{14}a_{49} - a_{15}a_{48}) - (a_{16}a_{47} - a_{17}a_{46}). \end{aligned}$$

By solving the complicated matrix equation in (2.7) by using MATHEMATICA, we obtain the amplitudes a_i . Each a_i is an algebraic sum of 64 terms being of the form $b_j\alpha_k\beta_l\gamma_m\delta_s\sigma_t\tau_h$. Then, by substituting a_i into $IV(a, 6)$, we obtain the following.

$$IV(a, 6) = IV(b, 6) \det(\alpha) \det(\beta) \det(\gamma) \det(\delta) \det(\sigma) \det(\tau). \quad (2.8)$$

Version 2 of the invariant

Definition

$sign^*(2, 0) = 1$. When $n \geq 3$, $sign^*(n, i) = sign(n, i)$ whenever $0 \leq i \leq 2^{n-3} - 1$ and $sign^*(n, i) = sign(n, 2^{n-2} - 1 - i)$ whenever $2^{n-3} - 1 < i \leq 2^{n-2} - 1$.

When $n \geq 2$, let

$$IV^*(a, n) = \sum_{i=0}^{2^{n-2}-1} sign^*(n, i)(a_{2i}a_{(2^n-1)-2i} - a_{2i+1}a_{(2^n-2)-2i}). \quad (2.9)$$

Clearly, when $n \geq 4$, $IV(a, n) = IV^*(a, n)$.

Thus, Theorem 1 can be rephrased as follows.

For $n(\geq 2)$ -qubits,

$$IV^*(a, n) = IV^*(b, n) \underbrace{\det(\alpha) \det(\beta) \det(\gamma) \dots}_n, \quad (2.10)$$

where $IV^*(b, n)$ is obtained from $IV^*(a, n)$ by replacing a in $IV^*(a, n)$ by b .

When $n = 2, 4$ and 6 , (2.10) is reduced to (2.2), (2.4) and (2.8), respectively. $IV^*(b, n)$ is another version of the invariant for even n -qubits.

2.2 The SLOCC invariant for odd n -qubits

2.2.1 For 3-qubits

If $|\psi\rangle$ and $|\psi'\rangle$ are equivalent under SLOCC, then they satisfy the following equation,

$$\begin{aligned} & ((a_0a_7 - a_1a_6) - (a_2a_5 - a_3a_4))^2 - 4(a_0a_3 - a_1a_2)(a_4a_7 - a_5a_6) = \\ & [((b_0b_7 - b_1b_6) - (b_2b_5 - b_3b_4))^2 - 4(b_0b_3 - b_1b_2)(b_4b_7 - b_5b_6)] \det(\alpha)^2 \det(\beta)^2 \det(\gamma)^2. \end{aligned} \quad (2.11)$$

The above equation can be equivalently replaced by one of the following two equations.

$$\begin{aligned} & (1).((a_0a_7 - a_3a_4) + (a_1a_6 - a_2a_5))^2 - 4(a_3a_5 - a_1a_7)(a_2a_4 - a_0a_6) = \\ & (((b_0b_7 - b_3b_4) + (b_1b_6 - b_2b_5))^2 - 4(b_3b_5 - b_1b_7)(b_2b_4 - b_0b_6)) \det(\alpha)^2 \det(\beta)^2 \det(\gamma)^2; \\ & (2).(a_0a_7 - a_3a_4 - (a_1a_6 - a_2a_5))^2 - 4(a_1a_4 - a_0a_5)(a_3a_6 - a_2a_7) = \\ & (b_0b_7 - b_3b_4 - (b_1b_6 - b_2b_5))^2 - 4(b_1b_4 - b_0b_5)(b_3b_6 - b_2b_7) \det(\alpha)^2 \det(\beta)^2 \det(\gamma)^2. \end{aligned}$$

Let $\overline{IV}(a, 3) = (a_0a_7 - a_1a_6) - (a_2a_5 - a_3a_4)$, $IV^*(a, 2) = a_0a_3 - a_1a_2$ and $IV_{+4}^*(a, 2) = (a_4a_7 - a_5a_6)$. Then, (2.11) can be rewritten as

$$(\overline{IV}(a, 3))^2 - 4IV^*(a, 2)IV_{+4}^*(a, 2) = [(\overline{IV}(b, 3))^2 - 4IV^*(b, 2)IV_{+4}^*(b, 2)] \det^2(\alpha) \det^2(\beta) \det^2(\gamma), \quad (2.12)$$

where $\overline{IV}(b, 3)$, $IV^*(b, 2)$ and $IV_{+4}^*(b, 2)$ are obtained from $\overline{IV}(a, 3)$, $IV^*(a, 2)$ and $IV_{+4}^*(a, 2)$ by replacing a by b , respectively.

In Appendix B of this paper, we give a formal proof of (2.12). The ideas for the proof will be used to by induction show the following Theorem 2.

By (2.12), $(\overline{IV}(b, 3))^2 - 4IV^*(b, 2)IV_{+4}^*(b, 2)$ does not vary when $\det^2(\alpha) \det^2(\beta) \det^2(\gamma) = 1$ or vanish under SLOCC operators.

2.2.2 For 5-qubits

So far, no one has reported the invariant for 5-qubits. Therefore, it is worth listing the explicit expression of the invariant for 5-qubits to understand the complicated expression of the invariant for odd n -qubits which is manifested below.

$|\psi\rangle$ and $|\psi'\rangle$ are equivalent under SLOCC if and only if there exist invertible local operators $\alpha, \beta, \gamma, \delta$ and σ such that

$$|\psi\rangle = \alpha \otimes \beta \otimes \gamma \otimes \delta \otimes \sigma |\psi'\rangle. \quad (2.13)$$

Let

$$\begin{aligned} A^* = & [-(a_2a_{29} - a_3a_{28} - a_{12}a_{19} + a_{13}a_{18}) - (a_4a_{27} - a_5a_{26} - a_{10}a_{21} + a_{11}a_{20}) \\ & + (a_0a_{31} - a_1a_{30} - a_{14}a_{17} + a_{15}a_{16}) + (a_6a_{25} - a_7a_{24} - a_8a_{23} + a_9a_{22})]^2 \\ & - 4[(a_0a_{15} - a_1a_{14}) + (a_6a_9 - a_7a_8) - (a_2a_{13} - a_3a_{12}) - (a_4a_{11} - a_5a_{10})] \\ & [(a_{16}a_{31} - a_{17}a_{30}) + (a_{22}a_{25} - a_{23}a_{24}) - (a_{18}a_{29} - a_{19}a_{28}) - (a_{20}a_{27} - a_{21}a_{26})] \end{aligned}$$

and let B^* be obtained from A^* by replacing a in A^* by b .

Then if $|\psi\rangle$ and $|\psi'\rangle$ are equivalent under SLOCC, then the amplitudes of the two states satisfy the following equation,

$$A^* = B^* * \det^2(\alpha) \det^2(\beta) \det^2(\gamma) \det^2(\delta) \det^2(\sigma). \quad (2.14)$$

We have verified (2.14) by using MATHEMATICA. That is, by solving the complicated matrix equation in (2.13), we obtain the amplitudes a_i . Each a_i is an algebraic sum of 32 terms being of the form $b_j\alpha_k\beta_l\gamma_m\delta_s\sigma_t$. Then, by substituting a_i into A^* , we obtain (2.14). However, this verification is helpless to finding a formal proof of the following Theorem 2. Hence, it is necessary to give a formal argument of (2.14) for readers to readily follow the complicated deduction in Appendix D of the following Theorem 2. The formal argument of (2.14) is put in Appendix C and gives hints which are used to by induction prove the following Theorem 2.

By (2.14), B^* does not vary when $\det^2(\alpha) \det^2(\beta) \det^2(\gamma) \det^2(\delta) \det^2(\sigma) = 1$ or vanish under SLOCC operators.

2.2.3 The definition and proof of SLOCC invariant for odd n -qubits

Let $|\psi\rangle$ and $|\psi'\rangle$ be any pure states of $n(\geq 3)$ -qubits. Let

$$\begin{aligned} \overline{IV}(a, n) = & \sum_{i=0}^{2^{n-3}-1} \text{sign}(n, i) [(a_{2i}a_{(2^n-1)-2i} - a_{2i+1}a_{(2^n-2)-2i}) \\ & - (a_{(2^{n-1}-2)-2i}a_{(2^{n-1}+1)+2i} - a_{(2^{n-1}-1)-2i}a_{2^{n-1}+2i})]. \end{aligned} \quad (2.15)$$

Let $IV_{+2^{n-1}}^*(a, n-1)$ be obtained from $IV^*(a, n-1)$ by adding 2^{n-1} to the subscripts in $IV^*(a, n-1)$ as follows.

$$IV_{+2^{n-1}}^*(a, n-1) = \sum_{i=0}^{2^{n-3}-1} \text{sign}^*(n-1, i)(a_{2^{n-1}+2i}a_{(2^n-1)-2i} - a_{2^{n-1}+1+2i}a_{(2^n-2)-2i}).$$

For example, $IV^*(a, 2) = a_0a_3 - a_1a_2$. Then $IV_{+4}^*(a, 2) = a_4a_7 - a_5a_6$.

Theorem 2.

Assume that $|\psi\rangle$ and $|\psi'\rangle$ are equivalent under SLOCC. Then the amplitudes of the two states satisfy the following equation,

$$\begin{aligned} (\overline{IV}(a, n))^2 - 4IV^*(a, n-1)IV_{+2^{n-1}}^*(a, n-1) = \\ [(\overline{IV}(b, n))^2 - 4IV^*(b, n-1)IV_{+2^{n-1}}^*(b, n-1)] \underbrace{\det^2(\alpha) \det^2(\beta) \det^2(\gamma) \dots}_n, \end{aligned} \quad (2.16)$$

where $IV^*(b, n-1)$ and $IV_{+2^{n-1}}^*(b, n-1)$ are obtained from $IV^*(a, n-1)$ and $IV_{+2^{n-1}}^*(a, n-1)$ by replacing a by b , respectively.

An inductive proof of Theorem 2 is put in Part 2 of Appendix D. When $n = 3$ and 5 , (2.16) becomes (2.12) and (2.14), respectively.

(2.16) declares that $(\overline{IV}(b, n))^2 - 4IV^*(b, n-1)IV_{+2^{n-1}}^*(b, n-1)$ does not vary when $\det^2(\alpha) \det^2(\beta) \det^2(\gamma) \dots = 1$ or vanish under SLOCC operators. Here, $(\overline{IV}(b, n))^2 - 4IV^*(b, n-1)IV_{+2^{n-1}}^*(b, n-1)$ is called as an invariant of odd n -qubits.

3 The residual entanglement for n -qubits

Coffman et al. [16] defined the residual entanglement for 3-qubits. We propose the residual entanglement for n -qubits as follows.

3.1 The residual entanglement for even n -qubits

Wong and Nelson's n -tangle for even n -qubits is listed as follows. See (2) in [18].

$$\tau_{1\dots n} = 2 \left| \sum a_{\alpha_1 \dots \alpha_n} a_{\beta_1 \dots \beta_n} a_{\gamma_1 \dots \gamma_n} a_{\delta_1 \dots \delta_n} \times \epsilon_{\alpha_1 \beta_1} \epsilon_{\alpha_2 \beta_2} \dots \epsilon_{\alpha_{n-1} \beta_{n-1}} \epsilon_{\gamma_1 \delta_1} \epsilon_{\gamma_2 \delta_2} \dots \times \epsilon_{\gamma_{n-1} \delta_{n-1}} \epsilon_{\alpha_n \gamma_n} \epsilon_{\beta_n \delta_n} \right|.$$

The n -tangle requires $3 * 2^{4n}$ multiplications.

When n is even, by means of (2.9), i.e., the invariant for even n -qubits, we define that for any state $|\psi\rangle$, the residual entanglement

$$\tau(\psi) = 2 |IV^*(a, n)|. \quad (3.1)$$

This residual entanglement requires 2^{n-1} multiplications. When $n = 2$, the residual entanglement $2 |IV^*(a, 2)|$ just is Coffman et al. 's concurrence $2\sqrt{\det \rho_A}$ [16].

From Theorem 1, we have the following corollary.

Corollary 1.

If $|\psi\rangle$ and $|\psi'\rangle$ are equivalent under SLOCC, then from (2.10),

$$\tau(\psi) = \tau(\psi') \underbrace{|\det(\alpha) \det(\beta) \det(\gamma) \dots|}_n. \quad (3.2)$$

It is straightforward to verify the following properties.

Lemma 1.

If a state of even n -qubits is a tensor product of a state of 1-qubit and a state of $(n-1)$ -qubits, then $\tau = 0$.

In particular, if a state of even n -qubits is full separable, then $\tau = 0$.

Lemma 2.

For 4-qubits, if $|\psi\rangle$ is a tensor product of state $|\phi\rangle$ of 2-qubits and state $|\omega\rangle$ of 2-qubits, then $\tau(\psi) = \tau(\phi)\tau(\omega)$.

For 6-qubits, there are two cases.

Case 1. If $|\psi\rangle$ is a tensor product of state $|\phi\rangle$ of 2-qubits and state $|\omega\rangle$ of 4-qubits, then $\tau(\psi) = \tau(\phi)\tau(\omega)$.

Case 2. If $|\psi\rangle$ is a tensor product of state $|\phi\rangle$ of 3-qubits and state $|\omega\rangle$ of 3-qubits, then $\tau(\psi) = 0$.

Conjecture:

(1). If $|\psi\rangle$ is a tensor product of state $|\phi\rangle$ of *even*-qubits and state $|\omega\rangle$ of *even*-qubits, then $\tau(\psi) = \tau(\phi)\tau(\omega)$.

(2). If $|\psi\rangle$ is a tensor product of state $|\phi\rangle$ of *odd*-qubits and state $|\omega\rangle$ of *odd*-qubits, then $\tau(\psi) = 0$.

3.1.1 $\tau \leq 1$

$|IV^*(a, n)| \leq \sum_{j=0}^{2^{n-1}-1} |a_j a_{(2^n-1)-j}| \leq \frac{1}{2} \sum_{j=0}^{2^{n-1}-1} (|a_j|^2 + |a_{(2^n-1)-j}|^2) = \frac{1}{2}$. Therefore $\tau \leq 1$. When $\tau = 1$, $|a_j| = |a_{(2^n-1)-j}|$, where $j = 0, 1, \dots, 2^{n-1} - 1$.

3.2 The residual entanglement for odd n -qubits

Wong and Nelson did not discuss odd n -tangle[18]. When n is odd, by means of the invariant for odd n -qubits, we define that for any state $|\psi\rangle$, the residual entanglement

$$\tau(\psi) = 4|(\overline{IV}(a, n))^2 - 4IV^*(a, n-1)IV_{+2^{n-1}}^*(a, n-1)|. \quad (3.3)$$

When $n = 3$, this residual entanglement τ just is Coffman et al. 's residual entanglement or 3-tangle $\tau_{ABC} = 4|d_1 - 2d_2 + 4d_3|$ [16].

From Theorem 2, we have the following corollary.

Corollary 2.

If $|\psi\rangle$ and $|\psi'\rangle$ are equivalent under SLOCC, then by Theorem 2, we obtain

$$\tau(\psi) = \tau(\psi') \underbrace{|\det(\alpha) \det(\beta) \det(\gamma) \dots|}_n. \quad (3.4)$$

The following results follow the definition of the residual entanglement immediately.

Lemma 3.

If a state of odd n -qubits is a tensor product of a state of 1-qubit and a state of $(n-1)$ -qubits, then $\tau = 0$.

In particular, if a state of odd n -qubits is full separable, then $\tau = 0$.

3.2.1 $\tau \leq 1$

The fact can be shown by computing the extremes. See Appendix E for the details. When $\tau = 1$, $|a_j| = |a_{(2^n-1)-j}|$, where $j = 0, 1, \dots, 2^{n-1} - 1$.

3.3 The invariant residual entanglement

Corollaries 1 and 2 imply that the residual entanglement does not vary when $|\det(\alpha) \det(\beta) \det(\gamma) \dots| = 1$ or vanish under SLOCC operators. Also, from Corollaries 1 and 2, it is easy to see that if $|\psi\rangle$ and $|\psi'\rangle$ are equivalent under SLOCC, then either $\tau(\psi) = \tau(\psi') = 0$ or $\tau(\psi)\tau(\psi') \neq 0$. Otherwise, the two states belong to different SLOCC classes.

3.4 States with the maximal residual entanglement

(1). Let state $|GHZ\rangle$ of n -qubits be $(|\underbrace{0\dots 0}_n\rangle + |\underbrace{1\dots 1}_n\rangle)/\sqrt{2}$. Then, no matter how n is even or odd, it is easy to see that $\tau = 1$ for state $|GHZ\rangle$ of n -qubits. We have shown that $\tau \leq 1$. Therefore, state $|GHZ\rangle$ has the maximal residual entanglement, i.e., $\tau = 1$. Also, $\tau = 1$ for any state of n -qubits which is equivalent to $|GHZ\rangle$ under determinant one SLOCC operations.

(2). There are many true entangled states with the maximal residual entanglement.

For example, when $n = 4$, $|C\rangle = (|3\rangle + |5\rangle + |6\rangle + |9\rangle + |10\rangle + |12\rangle)/\sqrt{6}$ [13]. $\tau(C) = 1$. As well, $\tau = 1$ for any state of 4-qubits which is equivalent to $|C\rangle$ under determinant one SLOCC operations.

(3) There are many product states with the maximal residual entanglement.

When $n = 4$, $\tau = 1$ for any state which is equivalent to $|GHZ\rangle_{12} \otimes |GHZ\rangle_{34}$, $|GHZ\rangle_{13} \otimes |GHZ\rangle_{24}$ or $|GHZ\rangle_{14} \otimes |GHZ\rangle_{23}$ under determinant one SLOCC operations.

When $n = 6$, $|GHZ\rangle_{12} \otimes |GHZ\rangle_{3456}$ and $|GHZ\rangle_{12} \otimes |GHZ\rangle_{34} \otimes |GHZ\rangle_{56}$ have the maximal residual entanglement $\tau = 1$.

The examples above illustrate that the residual entanglement is not the n -way entanglement.

3.5 The true entanglement classes with the minimal residual entanglement

(1). For state $|W\rangle$ of n -qubits, no matter how n is even (≥ 4) or odd (≥ 3), $\tau(W) = 0$. By Corollaries 1 and 2, $\tau = 0$ for any state which is equivalent to $|W\rangle$ under SLOCC.

(2). For 4-qubits, there are many true SLOCC entanglement classes which have the minimal residual entanglement $\tau = 0$ [13].

4 SLOCC classification

We used the invariant, D -criteria and F -criteria for SLOCC classification of 4-qubits [14]. The invariant and residual entanglement for n -qubits and the following D -criteria and F -criteria for n -qubits can be used for SLOCC classification of n -qubits. In this section, we also show that the dual states are SLOCC equivalent.

4.1 D -criteria for $n \geq 4$ -qubits

$$\begin{aligned} D_1^{(i)} &= (a_{1+8i}a_{4+8i} - a_{0+8i}a_{5+8i})(a_{2^n-8i-5}a_{2^n-8i-2} - a_{2^n-8i-6}a_{2^n-8i-1}) \\ &\quad - (a_{3+8i}a_{6+8i} - a_{2+8i}a_{7+8i})(a_{2^n-8i-7}a_{2^n-8i-4} - a_{2^n-8i-8}a_{2^n-8i-3}), \\ D_2^{(i)} &= (a_{4+8i}a_{7+8i} - a_{5+8i}a_{6+8i})(a_{2^n-8i-8}a_{2^n-8i-5} - a_{2^n-8i-7}a_{2^n-8i-6}) \\ &\quad - (a_{0+8i}a_{3+8i} - a_{1+8i}a_{2+8i})(a_{2^n-8i-4}a_{2^n-8i-1} - a_{2^n-8i-3}a_{2^n-8i-2}), \\ D_3^{(i)} &= (a_{3+8i}a_{5+8i} - a_{1+8i}a_{7+8i})(a_{2^n-8i-6}a_{2^n-8i-4} - a_{2^n-8i-8}a_{2^n-8i-2}) \\ &\quad - (a_{2+8i}a_{4+8i} - a_{0+8i}a_{6+8i})(a_{2^n-8i-5}a_{2^n-8i-3} - a_{2^n-8i-7}a_{2^n-8i-1}) \\ i &= 0, 1, \dots, 2^{n-4} - 1. \end{aligned}$$

4.2 F -criteria

When $i + j$ is odd,

$$(a_i a_j + a_k a_l - a_p a_q - a_r a_s)^2 - 4(a_i a_{j-1} - a_p a_{q-1})(a_k a_{l+1} - a_r a_{s+1}).$$

Otherwise,

$$(a_i a_j + a_k a_l - a_p a_q - a_r a_s)^2 - 4(a_i a_{j-2} - a_p a_{q-2})(a_k a_{l+2} - a_r a_{s+2}).$$

The subscripts above satisfy the following conditions.

$$\begin{aligned} i < j, k < l, p < q, r < s, i < k < p < r \\ i + j = k + l = p + q = r + s, i \oplus j = k \oplus l = p \oplus q = r \oplus s. \end{aligned} \quad (4.1)$$

For example, F -criteria include expressions in which $i + j = 7, 11, 13, 15, 17, 19$ and 23 and the expressions in which $i + j = 14$ and 16 , exclude the expressions in which $i + j = 8, 9, 10, 12, 18, 20, 21$ or 22 .

4.3 The dual states are SLOCC equivalent

Let $\bar{1}$ ($\bar{0}$) be the complement of a bit 1 (0). Then $\bar{0} = 1$ and $\bar{1} = 0$. Let $\bar{z} = \bar{z}_1 \bar{z}_2 \dots \bar{z}_n$ denote the complement of a binary string $z = z_1 z_2 \dots z_n$. Also, the set of the basis states $B = \{|\bar{0}\rangle, |\bar{1}\rangle, \dots, |\bar{2^n - 1}\rangle\}$. Let $|\varphi\rangle$ be any state of n -qubits. Then we can write $|\varphi\rangle = c_0|0\rangle + c_1|1\rangle + \dots + c_{2^n-1}|(2^n - 1)\rangle$. Let $|\bar{\varphi}\rangle = c_0|\bar{0}\rangle + c_1|\bar{1}\rangle + \dots + c_{2^n-1}|\bar{(2^n - 1)}\rangle$. We call $|\bar{\varphi}\rangle$ the complement of $|\varphi\rangle$.

Let $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then $\sigma_x \otimes \dots \otimes \sigma_x |\varphi\rangle = \sum_{i=0}^{2^n-1} c_i (\sigma_x \otimes \dots \otimes \sigma_x |i\rangle) = \sum_{i=0}^{2^n-1} c_i |\bar{i}\rangle = |\bar{\varphi}\rangle$.

Consequently, if two states of n -qubits are dual then they are SLOCC equivalent.

5 Summary

In this paper, we report the invariant for n -qubits. The invariant is only related to the amplitudes of the related two states and the determinants of the related operators. It reveals the inherent properties of SLOCC equivalence. By means of the invariant we propose the residual entanglement for n -qubits. When $n = 2$, it becomes Coffman et al.'s concurrence for 2-qubits and when $n = 3$, it is 3-tangle. For even n -qubits, it is much simpler than Wong and Nelson's even n -tangle[18]. For odd n -qubits, it requires 2^n multiplications. Wong and Nelson did not define the odd n -tangle. The properties of the residual entanglement are discussed in this paper. Wong and Nelson indicated out that when n is even, n -qubit $|GHZ\rangle$ state has the maximal n -tangle and n -qubit $|W\rangle$ state has the minimal n -tangle[18]. The present paper gives many true entangled states with the maximal residual entanglement: $\tau = 1$ and many true SLOCC entanglement classes with the minimal residual entanglement: $\tau = 0$. Wong and Nelson indicated out that their even n -tangle is not the n -way entanglement[18]. In the present paper, the properties of the residual entanglement claim that no matter how n is even or odd, the residual entanglement is not the n -way entanglement. The invariant and the residual entanglement can be used for SLOCC entanglement classification for n -qubits.

Appendix A: The proof of the invariant for 4-qubits

Let us prove (2.4). We can rewrite

$$|\Psi\rangle = |0\rangle \otimes \sum_{i=0}^7 (\alpha_1 d_i + \alpha_2 d_{8+i}) |i\rangle + |1\rangle \otimes \sum_{i=0}^7 (\alpha_3 d_i + \alpha_4 d_{8+i}) |i\rangle,$$

where

$$a_i = \alpha_1 d_i + \alpha_2 d_{8+i} \quad \text{and} \quad a_{8+i} = \alpha_3 d_i + \alpha_4 d_{8+i}, 0 \leq i \leq 7, \quad (\text{A1})$$

$$\sum_{i=0}^7 d_i |i\rangle = \beta \otimes \gamma \otimes \delta \sum_{i=0}^7 b_i |i\rangle, \quad (\text{A2})$$

$$\sum_{i=0}^7 d_{8+i} |i\rangle = \beta \otimes \gamma \otimes \delta \sum_{i=0}^7 b_{8+i} |i\rangle. \quad (\text{A3})$$

Notice that from (A2) and (A3) it happens that $\sum_{i=0}^{15} d_i |i\rangle = I \otimes \beta \otimes \gamma \otimes \delta \sum_{i=0}^{15} b_i |i\rangle$, where I is an identity.

(2.4) follows the following Steps 1 and 2 obviously.

Step 1. Prove $IV(a, 4) = IV(d, 4) \det(\alpha)$, where $IV(d, 4)$ is obtained from $IV(a, 4)$ by replacing a by d . From (A1), by computing,

$$(a_2 a_{13} - a_3 a_{12}) + (a_4 a_{11} - a_5 a_{10}) = [(d_2 d_{13} - d_3 d_{12}) + (d_4 d_{11} - d_5 d_{10})] \det(\alpha),$$

$$(a_0 a_{15} - a_1 a_{14}) + (a_6 a_9 - a_7 a_8) = [(d_0 d_{15} - d_1 d_{14}) + (d_6 d_9 - d_7 d_8)] \det(\alpha).$$

So the proof of Step 1 is done.

Step 2. Prove that

$$IV(d, 4) = IV(b, 4) \det(\beta) \det(\gamma) \det(\delta).$$

We can rewrite (A2) as

$$\sum_{i=0}^7 d_i |i\rangle = |0\rangle \otimes \sum_{i=0}^3 (\beta_1 h_i + \beta_2 h_{4+i}) |i\rangle + |1\rangle \otimes \sum_{i=0}^3 (\beta_3 h_i + \beta_4 h_{4+i}) |i\rangle, \quad (\text{A4})$$

where

$$\sum_{i=0}^3 h_i |i\rangle = \gamma \otimes \delta \sum_{i=0}^3 b_i |i\rangle, \quad (\text{A5})$$

$$\sum_{i=0}^3 h_{4+i} |i\rangle = \gamma \otimes \delta \sum_{i=0}^3 b_{4+i} |i\rangle, \quad (\text{A6})$$

$$d_i = \beta_1 h_i + \beta_2 h_{4+i} \quad \text{and} \quad d_{4+i} = \beta_3 h_i + \beta_4 h_{4+i}, 0 \leq i \leq 3. \quad (\text{A7})$$

Similarly, (A3) can be rewritten as

$$\sum_{i=0}^7 d_{8+i} |i\rangle = |0\rangle \otimes \sum_{i=0}^3 (\beta_1 h_{8+i} + \beta_2 h_{12+i}) |i\rangle + |1\rangle \otimes \sum_{i=0}^3 (\beta_3 h_{8+i} + \beta_4 h_{12+i}) |i\rangle,$$

where

$$\sum_{i=0}^3 h_{8+i} |i\rangle = \gamma \otimes \delta \sum_{i=0}^3 b_{8+i} |i\rangle, \quad (\text{A8})$$

$$\sum_{i=0}^3 h_{12+i} |i\rangle = \gamma \otimes \delta \sum_{i=0}^3 b_{12+i} |i\rangle, \quad (\text{A9})$$

$$d_{8+i} = \beta_1 h_{8+i} + \beta_2 h_{12+i} \quad \text{and} \quad d_{12+i} = \beta_3 h_{8+i} + \beta_4 h_{12+i}, 0 \leq i \leq 3. \quad (\text{A10})$$

By substituting (A7) and (A10) into $IV(d, 4)$,

$$IV(d, 4) = IV(h, 4) \det(\beta), \quad (\text{A11})$$

where $IV(h, 4)$ is obtained from $IV(a, 4)$ by replacing a by h .

From (A5) and (A6),

$$\sum_{i=0}^7 h_i |i\rangle = I \otimes \gamma \otimes \delta \sum_{i=0}^7 b_i |i\rangle. \quad (\text{A12})$$

From (A8) and (A9),

$$\sum_{i=0}^7 h_{8+i} |i\rangle = I \otimes \gamma \otimes \delta \sum_{i=0}^7 b_{8+i} |i\rangle. \quad (\text{A13})$$

From (A12) and (A13),

$$\sum_{i=0}^{15} h_i |i\rangle = I \otimes I \otimes \gamma \otimes \delta \sum_{i=0}^{15} b_i |i\rangle. \quad (\text{A14})$$

Similarly, from (A14) we can derive

$$IV(h, 4) = IV(b, 4) \det(\gamma) \det(\delta). \quad (\text{A15})$$

From (A11) and (A15), the proof of Step 2 is done.

Appendix B: The proof of the invariant for 3-qubits

We can rewrite

$$|\Psi\rangle = |0\rangle \otimes \sum_{i=0}^3 (\alpha_1 d_i + \alpha_2 d_{4+i}) |i\rangle + |1\rangle \otimes \sum_{i=0}^3 (\alpha_3 d_i + \alpha_4 d_{4+i}) |i\rangle,$$

where

$$a_i = \alpha_1 d_i + \alpha_2 d_{4+i} \quad \text{and} \quad a_{4+i} = \alpha_3 d_i + \alpha_4 d_{4+i}, 0 \leq i \leq 3, \quad (\text{B1})$$

$$\sum_{i=0}^3 d_i |i\rangle = \beta \otimes \gamma \sum_{i=0}^3 b_i |i\rangle, \quad (\text{B2})$$

$$\sum_{i=0}^3 d_{4+i} |i\rangle = \beta \otimes \gamma \sum_{i=0}^3 b_{4+i} |i\rangle. \quad (\text{B3})$$

Notice that from (B2) and (B3) it happens that $\sum_{i=0}^7 d_i |i\rangle = I \otimes \beta \otimes \gamma \sum_{i=0}^7 b_i |i\rangle$, where I is an identity. (2.12) can be obtained from the following Steps 1 and 2.

Step 1. Prove that

$$(\overline{IV}(a, 3))^2 - 4IV^*(a, 2)IV_{+4}^*(a, 2) = [(\overline{IV}(d, 3))^2 - 4IV^*(d, 2)IV_{+4}^*(d, 2)] \det(\alpha)^2,$$

where $\overline{IV}(d, 3)$, $IV^*(d, 2)$ and $IV_{+4}^*(d, 2)$ are obtained from $\overline{IV}(a, 3)$, $IV^*(a, 2)$ and $IV_{+4}^*(a, 2)$ by replacing a by d , respectively.

From (B1), by computing,

$$IV^*(a, 2) = IV^*(d, 2)\alpha_1^2 + \overline{IV}(d, 3)\alpha_1\alpha_2 + IV_{+4}^*(d, 2)\alpha_2^2, \quad (\text{B4})$$

$$IV_{+4}^*(a, 2) = IV^*(d, 2)\alpha_3^2 + \overline{IV}(d, 3)\alpha_3\alpha_4 + IV_{+4}^*(d, 2)\alpha_4^2, \quad (\text{B5})$$

$$\overline{IV}(a, 3) = 2IV^*(d, 2)\alpha_1\alpha_3 + \overline{IV}(d, 3)(\alpha_1\alpha_4 + \alpha_2\alpha_3) + 2IV_{+4}^*(d, 2)\alpha_2\alpha_4. \quad (\text{B6})$$

Then the proof of Step 1 follows (B4), (B5) and (B6) straightforwardly.

Step 2. Prove that

$$(\overline{IV}(d, 3))^2 - 4IV^*(d, 2)IV_{+4}^*(d, 2) = [(\overline{IV}(b, 3))^2 - 4IV^*(b, 2)IV_{+4}^*(b, 2)] \det(\beta)^2 \det(\gamma)^2.$$

By (2.2), from (B2),

$$IV^*(d, 2) = IV^*(b, 2) \det(\beta) \det(\gamma), \quad (\text{B7})$$

and from (B3),

$$IV_{+4}^*(d, 2) = IV_{+4}^*(b, 2) \det(\beta) \det(\gamma). \quad (\text{B8})$$

Let us compute $\overline{IV}(d, 3)$. From (B2) and (B3) we obtain

$$\sum_{i=0}^3 (d_i - d_{4+i}) |i\rangle = \beta \otimes \gamma \sum_{i=0}^3 (b_i - b_{4+i}) |i\rangle. \quad (\text{B9})$$

By (2.2), from (B9) it is easy to see

$$(d_0 - d_4)(d_3 - d_7) - (d_1 - d_5)(d_2 - d_6) = [(b_0 - b_4)(b_3 - b_7) - (b_1 - b_5)(b_2 - b_6)] \det(\beta) \det(\gamma). \quad (\text{B10})$$

Expanding (B10), we have

$$IV^*(d, 2) + IV_{+4}^*(d, 2) - \overline{IV}(d, 3) = [IV^*(b, 2) + IV_{+4}^*(b, 2) - \overline{IV}(b, 3)] \det(\beta) \det(\gamma). \quad (\text{B11})$$

From (B7), (B8) and (B11), we get

$$\overline{IV}(d, 3) = \overline{IV}(b, 3) \det(\beta) \det(\gamma). \quad (\text{B12})$$

The proof of Step 2 follows (B7), (B8) and (B12) immediately.

Appendix C: The proof of the invariant for 5-qubits

$|\psi'\rangle$ can be rewritten as

$$|\psi'\rangle = |0\rangle \otimes \sum_{i=0}^{15} b_i |i\rangle + |1\rangle \otimes \sum_{i=0}^{15} b_{16+i} |i\rangle.$$

Thus,

$$|\psi\rangle = \alpha |0\rangle \otimes \beta \otimes \gamma \otimes \delta \otimes \sigma \sum_{i=0}^{15} b_i |i\rangle + \alpha |1\rangle \otimes \beta \otimes \gamma \otimes \delta \otimes \sigma \sum_{i=0}^{15} b_{16+i} |i\rangle.$$

Let

$$\sum_{i=0}^{15} d_i |i\rangle = \beta \otimes \gamma \otimes \delta \otimes \sigma \sum_{i=0}^{15} b_i |i\rangle \quad (C1)$$

and

$$\sum_{i=0}^{15} d_{16+i} |i\rangle = \beta \otimes \gamma \otimes \delta \otimes \sigma \sum_{i=0}^{15} b_{16+i} |i\rangle. \quad (C2)$$

By (C1) and (C2), we can rewrite

$$|\psi\rangle = (\alpha_1 |0\rangle + \alpha_3 |1\rangle) \otimes \sum_{i=0}^{15} d_i |i\rangle + (\alpha_2 |0\rangle + \alpha_4 |1\rangle) \otimes \sum_{i=0}^{15} d_{16+i} |i\rangle. \quad (C3)$$

From (C3), we have

$$|\psi\rangle = |0\rangle \otimes \sum_{i=0}^{15} (\alpha_1 d_i + \alpha_2 d_{16+i}) |i\rangle + |1\rangle \otimes \sum_{i=0}^{15} (\alpha_3 d_i + \alpha_4 d_{16+i}) |i\rangle. \quad (C4)$$

From (C4), we can obtain the amplitudes

$$a_i = \alpha_1 d_i + \alpha_2 d_{16+i} \quad \text{and} \quad a_{16+i} = \alpha_3 d_i + \alpha_4 d_{16+i}, \quad (C5)$$

where $0 \leq i \leq 15$.

By substituting (C5) into A^* , we obtain

$$A^* = D^* \overset{2}{*} \det(\alpha),$$

where

$$\begin{aligned} D^* = \{ & [(d_2 d_{29} - d_3 d_{28} - d_{12} d_{19} + d_{13} d_{18}) + (d_4 d_{27} - d_5 d_{26} - d_{10} d_{21} + d_{11} d_{20}) \\ & - (d_0 d_{31} - d_1 d_{30} - d_{14} d_{17} + d_{15} d_{16}) - (d_6 d_{25} - d_7 d_{24} - d_8 d_{23} + d_9 d_{22})]^2 \\ & - 4[(d_0 d_{15} - d_1 d_{14}) + (d_6 d_9 - d_7 d_8) - (d_2 d_{13} - d_3 d_{12}) - (d_4 d_{11} - d_5 d_{10})] \\ & [(d_{16} d_{31} - d_{17} d_{30}) + (d_{22} d_{25} - d_{23} d_{24}) - (d_{18} d_{29} - d_{19} d_{28}) - (d_{20} d_{27} - d_{21} d_{26})] \}. \end{aligned}$$

Next let us show that

$$D^* = B^* \overset{2}{*} \det(\beta) \overset{2}{*} \det(\gamma) \overset{2}{*} \det(\delta) \overset{2}{*} \det(\sigma). \quad (C6)$$

From (C1) and by (2.4), we obtain

$$\begin{aligned}
& (d_0d_{15} - d_1d_{14}) + (d_6d_9 - d_7d_8) - (d_2d_{13} - d_3d_{12}) - (d_4d_{11} - d_5d_{10}) = \\
& [(b_0b_{15} - b_1b_{14}) + (b_6b_9 - b_7b_8) - (b_2b_{13} - b_3b_{12}) - (b_4b_{11} - b_5b_{10})] \\
& * \det(\beta) \det(\gamma) \det(\delta) \det(\sigma).
\end{aligned} \tag{C7}$$

From (C2) and by (2.4), we obtain

$$\begin{aligned}
& (d_{16}d_{31} - d_{17}d_{30}) + (d_{22}d_{25} - d_{23}d_{24}) - (d_{18}d_{29} - d_{19}d_{28}) - (d_{20}d_{27} - d_{21}d_{26}) = \\
& [(b_{16}b_{31} - b_{17}b_{30}) + (b_{22}b_{25} - b_{23}b_{24}) - (b_{18}b_{29} - b_{19}b_{28}) - (b_{20}b_{27} - b_{21}b_{26})] \\
& * \det(\beta) \det(\gamma) \det(\delta) \det(\sigma).
\end{aligned} \tag{C8}$$

From (C1) and (C2), we have

$$\sum_{i=0}^{15} (d_i - d_{16+i})|i\rangle = \beta \otimes \gamma \otimes \delta \otimes \sigma \sum_{i=0}^{15} (b_i - b_{16+i})|i\rangle. \tag{C9}$$

By (2.4), from (C9) we obtain

$$\begin{aligned}
& ((d_0 - d_{16})(d_{15} - d_{31}) - (d_1 - d_{17})(d_{14} - d_{30})) + ((d_6 - d_{22})(d_9 - d_{25}) - (d_7 - d_{23})(d_8 - d_{24})) \\
& - ((d_2 - d_{18})(d_{13} - d_{29}) - (d_3 - d_{19})(d_{12} - d_{28})) - ((d_4 - d_{20})(d_{11} - d_{27}) - (d_5 - d_{21})(d_{10} - d_{26})) = \\
& ((b_0 - b_{16})(b_{15} - b_{31}) - (b_1 - b_{17})(b_{14} - b_{30})) + ((b_6 - b_{22})(b_9 - b_{25}) - (b_7 - b_{23})(b_8 - b_{24})) \\
& - ((b_2 - b_{18})(b_{13} - b_{29}) - (b_3 - b_{19})(b_{12} - b_{28})) - ((b_4 - b_{20})(b_{11} - b_{27}) - (b_5 - b_{21})(b_{10} - b_{26})) \\
& * \det(\beta) \det(\gamma) \det(\delta) \det(\sigma).
\end{aligned} \tag{C10}$$

By expanding (C10) and using (C7) and (C8), we obtain

$$\begin{aligned}
& (d_2d_{29} - d_3d_{28} - d_{12}d_{19} + d_{13}d_{18}) + (d_4d_{27} - d_5d_{26} - d_{10}d_{21} + d_{11}d_{20}) \\
& - (d_0d_{31} - d_1d_{30} - d_{14}d_{17} + d_{15}d_{16}) - (d_6d_{25} - d_7d_{24} - d_8d_{23} + d_9d_{22}) = \\
& [(b_2b_{29} - b_3b_{28} - b_{12}b_{19} + b_{13}b_{18}) + (b_4b_{27} - b_5b_{26} - b_{10}b_{21} + b_{11}b_{20}) \\
& - (b_0b_{31} - b_1b_{30} - b_{14}b_{17} + b_{15}b_{16}) - (b_6b_{25} - b_7b_{24} - b_8b_{23} + b_9b_{22})] \\
& \det(\beta) \det(\gamma) \det(\delta) \det(\sigma).
\end{aligned} \tag{C11}$$

Then (C6) follows (C7), (C8) and (C11).

Finally, (2.14) follows (??) and (C6).

Appendix D: The proofs of the invariant for n -qubits

We can rewrite

$$|\Psi\rangle = |0\rangle \otimes \sum_{i=0}^{2^{n-1}-1} (\alpha_1 d_i + \alpha_2 d_{2^{n-1}+i})|i\rangle + |1\rangle \otimes \sum_{i=0}^{2^{n-1}-1} (\alpha_3 d_i + \alpha_4 d_{2^{n-1}+i})|i\rangle,$$

where

$$\begin{aligned}
& a_i = \alpha_1 d_i + \alpha_2 d_{2^{n-1}+i} \quad \text{and} \quad a_{2^{n-1}+i} = \alpha_3 d_i + \alpha_4 d_{2^{n-1}+i}, \\
& 0 \leq i \leq 2^{n-1} - 1,
\end{aligned} \tag{D1}$$

$$\sum_{i=0}^{2^{n-1}-1} d_i|i\rangle = \underbrace{\beta \otimes \gamma \otimes \dots}_{n-1} \sum_{i=0}^{2^{n-1}-1} b_i|i\rangle, \quad (D2)$$

$$\sum_{i=0}^{2^{n-1}-1} d_{2^{n-1}+i}|i\rangle = \underbrace{\beta \otimes \gamma \otimes \dots}_{n-1} \sum_{i=0}^{2^{n-1}-1} b_{2^{n-1}+i}|i\rangle. \quad (D3)$$

From (D2) and (D3), it happens that $\sum_{i=0}^{2^n-1} d_i|i\rangle = I \otimes \beta \otimes \gamma \dots \sum_{i=0}^{2^n-1} b_i|i\rangle$, where I is an identity. Lemma 1.

$$\begin{aligned} & (a_{2i}a_{(2^n-1)-2i} - a_{2i+1}a_{(2^n-2)-2i}) + (a_{(2^{n-1}-2)-2i}a_{(2^{n-1}+1)+2i} - a_{(2^{n-1}-1)-2i}a_{2^{n-1}+2i}) = \\ & (d_{2i}d_{(2^n-1)-2i} - d_{2i+1}d_{(2^n-2)-2i}) + (d_{(2^{n-1}-2)-2i}d_{(2^{n-1}+1)+2i} - d_{(2^{n-1}-1)-2i}d_{2^{n-1}+2i}) \\ & * \det(\alpha) \end{aligned} \quad (D4)$$

Proof.

By (D1),

$$\begin{aligned} a_{2i} &= \alpha_1 d_{2i} + \alpha_2 d_{2^{n-1}+2i}, \\ a_{(2^n-1)-2i} &= \alpha_3 d_{2^{n-1}-1-2i} + \alpha_4 d_{(2^n-1)-2i}, \\ a_{2i+1} &= \alpha_1 d_{2i+1} + \alpha_2 d_{2^{n-1}+2i+1}, \\ a_{(2^n-2)-2i} &= \alpha_3 d_{(2^{n-1}-2)-2i} + \alpha_4 d_{(2^n-2)-2i}. \end{aligned} \quad (D5)$$

By (D5),

$$\begin{aligned} & (a_{2i}a_{(2^n-1)-2i} - a_{2i+1}a_{(2^n-2)-2i}) = \\ & \alpha_1 \alpha_3 (d_{2i}d_{2^{n-1}-1-2i} - d_{2i+1}d_{(2^{n-1}-2)-2i}) \\ & + \alpha_1 \alpha_4 (d_{2i}d_{(2^n-1)-2i} - d_{2i+1}d_{(2^n-2)-2i}) \\ & + \alpha_2 \alpha_3 (d_{2^{n-1}+2i}d_{2^{n-1}-1-2i} - d_{2^{n-1}+2i+1}d_{(2^{n-1}-2)-2i}) \\ & + \alpha_2 \alpha_4 (d_{2^{n-1}+2i}d_{(2^n-1)-2i} - d_{2^{n-1}+2i+1}d_{(2^n-2)-2i}). \end{aligned} \quad (D6)$$

By (D1),

$$\begin{aligned} a_{(2^{n-1}-2)-2i} &= \alpha_1 d_{(2^{n-1}-2)-2i} + \alpha_2 d_{2^{n-2}-2i}, \\ a_{(2^{n-1}+1)+2i} &= \alpha_3 d_{2i+1} + \alpha_4 d_{2^{n-1}+2i}, \\ a_{(2^{n-1}-1)-2i} &= \alpha_1 d_{(2^{n-1}-1)-2i} + \alpha_2 d_{2^{n-1}-2i}, \\ a_{2^{n-1}+2i} &= \alpha_3 d_{2i} + \alpha_4 d_{2^{n-1}+2i}. \end{aligned} \quad (D7)$$

So, by (D7),

$$\begin{aligned} & (a_{(2^{n-1}-2)-2i}a_{(2^{n-1}+1)+2i} - a_{(2^{n-1}-1)-2i}a_{2^{n-1}+2i}) = \\ & -\alpha_1 \alpha_3 (d_{2i}d_{2^{n-1}-1-2i} - d_{2i+1}d_{(2^{n-1}-2)-2i}) \\ & + \alpha_1 \alpha_4 (d_{(2^{n-1}-2)-2i}d_{2^{n-1}+2i} - d_{(2^{n-1}-1)-2i}d_{2^{n-1}+2i}) \\ & + \alpha_2 \alpha_3 (d_{2i+1}d_{2^{n-2}-2i} - d_{2i}d_{2^{n-1}-2i}) \\ & - \alpha_2 \alpha_4 (d_{2^{n-1}+2i}d_{(2^n-1)-2i} - d_{2^{n-1}+2i+1}d_{(2^n-2)-2i}). \end{aligned} \quad (D8)$$

So, by (D6) and (D8),

$$\begin{aligned} & (a_{2i}a_{(2^n-1)-2i} - a_{2i+1}a_{(2^n-2)-2i}) + (a_{(2^{n-1}-2)-2i}a_{(2^{n-1}+1)+2i} - a_{(2^{n-1}-1)-2i}a_{2^{n-1}+2i}) = \\ & \alpha_1 \alpha_4 [(d_{2i}d_{(2^n-1)-2i} - d_{2i+1}d_{(2^n-2)-2i}) + (d_{(2^{n-1}-2)-2i}d_{2^{n-1}+2i} - d_{(2^{n-1}-1)-2i}d_{2^{n-1}+2i})] \\ & - \alpha_2 \alpha_3 [(d_{2i}d_{(2^n-1)-2i} - d_{2i+1}d_{(2^n-2)-2i}) + (d_{(2^{n-1}-2)-2i}d_{2^{n-1}+2i} - d_{(2^{n-1}-1)-2i}d_{2^{n-1}+2i})] = \\ & [(d_{2i}d_{(2^n-1)-2i} - d_{2i+1}d_{(2^n-2)-2i}) + (d_{(2^{n-1}-2)-2i}d_{(2^{n-1}+1)+2i} - d_{(2^{n-1}-1)-2i}d_{2^{n-1}+2i})] \\ & * \det(\alpha). \end{aligned}$$

Lemma 2.

When $0 \leq i \leq 2^{n-3} - 1$, $\text{sign}^*(n-1, i) = \text{sign}(n, i)$.

Proof. There are two cases.

Case 1. $0 \leq i \leq 2^{n-4} - 1$.

By the definitions, $\text{sign}^*(n-1, i) = \text{sign}(n-1, i)$ and $\text{sign}(n, i) = \text{sign}(n-1, i)$. Therefore for the case, $\text{sign}^*(n-1, i) = \text{sign}(n, i)$.

Case 2. $2^{n-4} - 1 < i \leq 2^{n-3} - 1$.

By the definitions $\text{sign}^*(n-1, i) = \text{sign}(n-1, 2^{n-3} - 1 - i)$ and $\text{sign}(n, i) = \text{sign}(n, 2^{n-3} - 1 - i)$ because n is odd. Since $0 \leq 2^{n-3} - 1 - i < 2^{n-4}$, by the definition $\text{sign}(n, 2^{n-3} - 1 - i) = \text{sign}(n-1, 2^{n-3} - 1 - i)$. Hence, $\text{sign}^*(n-1, i) = \text{sign}(n, i)$ for the case.

Consequently, the argument is done by Cases 1 and 2.

Part 1. The proof of Theorem 1 (for even n -qubits)

For the proof of the invariant for 4-qubits, see Appendix A. The proof of Theorem 1 follows the following Steps 1 and 2.

Step 1. Prove $IV(a, n) = IV(d, n) \det(\alpha)$, where $IV(d, n)$ is obtained from $IV(a, n)$ by replacing a by d . By lemma 1 above, clearly Step 1 holds.

Step 2. Prove $IV(d, n) = IV(b, n) \underbrace{\det(\beta) \det(\gamma) \dots}_{n-1}$.

Step 2.1. Prove $IV(d, n) = IV(h, n) \det(\beta)$, where $\sum_{i=0}^{2^n-1} h_i |i\rangle = \underbrace{I \otimes I \otimes \gamma \dots}_n \sum_{i=0}^{2^n-1} b_i |i\rangle$ and $IV(h, n)$

is obtained from $IV(a, n)$ by replacing a by h .

Notice that in Step 2.1 we will present the idea which will be used in the proof of Step 2.2 (for general case).

Proof.

From (D2),

$$\sum_{i=0}^{2^{n-1}-1} d_i |i\rangle = (\beta_1 |0\rangle + \beta_3 |1\rangle) \otimes \gamma \otimes \dots \sum_{i=0}^{2^{n-2}-1} b_i |i\rangle + (\beta_2 |0\rangle + \beta_4 |1\rangle) \otimes \gamma \otimes \dots \sum_{i=0}^{2^{n-2}-1} b_{2^{n-2}+i} |i\rangle. \quad (\text{D9})$$

Let

$$\sum_{i=0}^{2^{n-2}-1} h_i |i\rangle = \gamma \otimes \dots \sum_{i=0}^{2^{n-2}-1} b_i |i\rangle \quad \text{and} \quad \sum_{i=0}^{2^{n-2}-1} h_{2^{n-2}+i} |i\rangle = \gamma \otimes \dots \sum_{i=0}^{2^{n-2}-1} b_{2^{n-2}+i} |i\rangle \quad (\text{D10})$$

Then (D9) can be rewritten as follows.

$$\sum_{i=0}^{2^{n-1}-1} d_i |i\rangle = |0\rangle \otimes \sum_{i=0}^{2^{n-2}-1} (\beta_1 h_i + \beta_2 h_{2^{n-2}+i}) |i\rangle + |1\rangle \otimes \sum_{i=0}^{2^{n-2}-1} (\beta_3 h_i + \beta_4 h_{2^{n-2}+i}) |i\rangle.$$

Thus

$$d_i = \beta_1 h_i + \beta_2 h_{2^{n-2}+i} \quad \text{and} \quad d_{2^{n-2}+i} = \beta_3 h_i + \beta_4 h_{2^{n-2}+i}, 0 \leq i \leq 2^{n-2} - 1. \quad (\text{D11})$$

As well, from (D3) we obtain

$$\begin{aligned} \sum_{i=0}^{2^{n-1}-1} d_{2^{n-1}+i} |i\rangle = \\ |0\rangle \otimes \sum_{i=0}^{2^{n-2}-1} (\beta_1 h_{2^{n-1}+i} + \beta_2 h_{2^{n-1}+2^{n-2}+i}) |i\rangle + |1\rangle \otimes \sum_{i=0}^{2^{n-2}-1} (\beta_3 h_{2^{n-1}+i} + \beta_4 h_{2^{n-1}+2^{n-2}+i}) |i\rangle, \end{aligned} \quad (\text{D12})$$

where

$$\sum_{i=0}^{2^{n-2}-1} h_{2^{n-1}+i}|i\rangle = \gamma \otimes \dots \sum_{i=0}^{2^{n-2}-1} b_{2^{n-1}+i}|i\rangle$$

and

$$\sum_{i=0}^{2^{n-2}-1} h_{2^{n-1}+2^{n-2}+i}|i\rangle = \gamma \otimes \dots \sum_{i=0}^{2^{n-2}-1} b_{2^{n-1}+2^{n-2}+i}|i\rangle \quad (\text{D13})$$

From (D12), we obtain

$$d_{2^{n-1}+i} = \beta_1 h_{2^{n-1}+i} + \beta_2 h_{2^{n-1}+2^{n-2}+i} \quad \text{and} \quad d_{2^{n-1}+2^{n-2}+i} = \beta_3 h_{2^{n-1}+i} + \beta_4 h_{2^{n-1}+2^{n-2}+i}, \quad (\text{D14})$$

where $0 \leq i \leq 2^{n-2} - 1$.

Note that from (D10) and (D13), clearly

$$\sum_{i=0}^{2^n-1} h_i|i\rangle = I \otimes I \otimes \gamma \otimes \dots \sum_{i=0}^{2^n-1} b_i|i\rangle.$$

Now we demonstrate $IV(d, n) = IV(h, n) \det(\beta)$.

To compute $IV(d, n)$, let

$$T(i) = (d_{2i}d_{(2^{n-1}-2i)} - d_{2i+1}d_{(2^{n-2}-2i)}) + (d_{(2^{n-1}-2)-2i}d_{(2^{n-1}+1)+2i} - d_{(2^{n-1}-1)-2i}d_{2^{n-1}+2i})$$

in (2.5).

Let us compute $T(i)$ by using (D11) and (D14). Then we obtain the coefficients of $\beta_1\beta_4, \beta_2\beta_3, \beta_1\beta_3$ and $\beta_2\beta_4$ in $T(i)$ as follows.

(1). The coefficients of $\beta_1\beta_4$ in $T(i)$ is

$$\text{sign}(n, i)[(h_{2i}h_{(2^{n-1}-2i)} - h_{2i+1}h_{(2^{n-2}-2i)}) + (h_{(2^{n-1}-2)-2i}h_{(2^{n-1}+1)+2i} - h_{(2^{n-1}-1)-2i}h_{2^{n-1}+2i})].$$

Then it is easy to see that the coefficient of $\beta_1\beta_4$ in $IV(d, n)$ is $IV(h, n)$.

(2). The coefficient of $\beta_2\beta_3$ in $T(i)$ is

$$\text{sign}(n, i)[(h_{2^{n-2}+2i}h_{3*2^{n-2}-1-2i} - h_{2i+1+2^{n-2}}h_{3*2^{n-2}-2-2i}) + (h_{(2^{n-2}-2)-2i}h_{3*2^{n-2}+1+2i} - h_{(2^{n-2}-1)-2i}h_{3*2^{n-2}+2i})].$$

Then, the coefficient of $\beta_2\beta_3$ in $IV(d, n)$ is

$$\sum_{i=0}^{2^{n-3}-1} \text{sign}(n, i)[(h_{2^{n-2}+2i}h_{3*2^{n-2}-1-2i} - h_{2i+1+2^{n-2}}h_{3*2^{n-2}-2-2i}) + (h_{(2^{n-2}-2)-2i}h_{3*2^{n-2}+1+2i} - h_{(2^{n-2}-1)-2i}h_{3*2^{n-2}+2i})].$$

Let $j = 2^{n-3} - 1 - i$. Note that $\text{sign}(n, 2^{n-3} - 1 - j) = -\text{sign}(n, j)$ by the definition. It is not hard to see that the coefficient of $\beta_2\beta_3$ in $IV(d, n)$ happens to be $-IV(h, n)$.

(3). The coefficient of $\beta_1\beta_3$ in $T(i)$ is

$$\text{sign}(n, i)[(h_{2i}h_{(3*2^{n-2}-1)-2i} - h_{2i+1}h_{(3*2^{n-2}-2)-2i}) + (h_{(2^{n-2}-2)-2i}h_{(2^{n-1}+1)+2i} - h_{(2^{n-2}-1)-2i}h_{2^{n-1}+2i})].$$

Note that the coefficient of $\beta_1\beta_3$ in $T(2^{n-3} - 1 - i)$ is the opposite number of the one of $\beta_1\beta_3$ in $T(i)$ because $\text{sign}(n, 2^{n-3} - 1 - i) = -\text{sign}(n, i)$. Therefore the coefficient of $\beta_1\beta_3$ in $IV(d, n)$ vanishes.

(4). The coefficient of $\beta_2\beta_4$ in $T(i)$ is

$$\text{sign}(n, i)[(h_{2^{n-2}+2i}h_{(2^{n-1}-2i)} - h_{2^{n-2}+2i+1}h_{(2^{n-2}-2i)}) + (h_{(2^{n-1}-2)-2i}h_{(3*2^{n-2}+1)+2i} - h_{(2^{n-1}-1)-2i}h_{3*2^{n-2}+2i})].$$

Note that the coefficient of $\beta_2\beta_4$ in $T(2^{n-3} - 1 - i)$ is the opposite number of the one of $\beta_2\beta_4$ in $T(i)$. As well, the coefficient of $\beta_2\beta_4$ in $IV(d, n)$ vanishes.

From the above discussion, it is straightforward that $IV(d, n) = IV(h, n) \det(\beta)$.

Step 2.2. For general case

Let

$$\sum_{i=0}^{2^n-1} p_i |i\rangle = \underbrace{I \otimes I \otimes \dots \otimes I}_l \otimes \underbrace{\tau \otimes \sigma \otimes \dots}_{n-l} \sum_{i=0}^{2^n-1} b_i |i\rangle.$$

Then $IV(p, n) = IV(r, n) \det(\tau)$, where

$$\sum_{i=0}^{2^n-1} r_i |i\rangle = \underbrace{I \otimes I \otimes \dots \otimes I}_{l+1} \otimes \underbrace{\sigma \otimes \dots}_{n-l-1} \sum_{i=0}^{2^n-1} b_i |i\rangle.$$

Note that $IV(p, n)$ and $IV(r, n)$ are obtained from $IV(a, n)$ by replacing a by p and r , respectively.

Proof.

We rewrite

$$\begin{aligned} \sum_{i=0}^{2^n-1} b_i |i\rangle &= |0\rangle_l \otimes \sum_{i=0}^{2^{n-l}-1} b_i |i\rangle_{n-l} + \dots + |k\rangle_l \otimes \sum_{i=0}^{2^{n-l}-1} b_{k*2^{n-l}+i} |i\rangle_{n-l} + \dots + |2^l-1\rangle_l \otimes \sum_{i=0}^{2^{n-l}-1} b_{(2^l-1)*2^{n-l}+i} |i\rangle_{n-l} \\ &= \sum_{k=0}^{2^l-1} (|k\rangle_l \otimes \sum_{i=0}^{2^{n-l}-1} b_{k*2^{n-l}+i} |i\rangle_{n-l}). \end{aligned}$$

Then

$$\sum_{i=0}^{2^n-1} p_i |i\rangle = \sum_{k=0}^{2^l-1} (|k\rangle_l \otimes \underbrace{\tau \otimes \sigma \otimes \dots}_{n-l} \sum_{i=0}^{2^{n-l}-1} b_{k*2^{n-l}+i} |i\rangle_{n-l}).$$

Thus, $\sum_{i=0}^{2^{n-l}-1} p_{k*2^{n-l}+i} |i\rangle = \underbrace{\tau \otimes \sigma \otimes \dots}_{n-l} \sum_{i=0}^{2^{n-l}-1} b_{k*2^{n-l}+i} |i\rangle_{n-l}$, where $0 \leq k \leq 2^l - 1$.

By the above discussion,

$$\begin{aligned} \sum_{i=0}^{2^{n-l}-1} p_{k*2^{n-l}+i} |i\rangle &= (\tau_1|0\rangle + \tau_3|1\rangle) \otimes \underbrace{\sigma \otimes \dots}_{n-l-1} \sum_{i=0}^{2^{n-l-1}-1} b_{k*2^{n-l}+i} |i\rangle_{n-l-1} \\ &+ (\tau_2|0\rangle + \tau_4|1\rangle) \otimes \underbrace{\sigma \otimes \dots}_{n-l-1} \sum_{i=0}^{2^{n-l-1}-1} b_{k*2^{n-l}+2^{n-l-1}+i} |i\rangle_{n-l-1}. \end{aligned} \quad (D15)$$

Let

$$\sum_{i=0}^{2^{n-l-1}-1} r_{k*2^{n-l}+i} |i\rangle = \underbrace{\sigma \otimes \dots}_{n-l-1} \sum_{i=0}^{2^{n-l-1}-1} b_{k*2^{n-l}+i} |i\rangle_{n-l-1}. \quad (D16)$$

and

$$\sum_{i=0}^{2^{n-l-1}-1} r_{k*2^{n-l}+2^{n-l-1}+i} |i\rangle = \underbrace{\sigma \otimes \dots}_{n-l-1} \sum_{i=0}^{2^{n-l-1}-1} b_{k*2^{n-l}+2^{n-l-1}+i} |i\rangle_{n-l-1}, \quad (D17)$$

where $0 \leq k \leq 2^l - 1$.

From (D16) and (D17), it is not hard to see that

$$\sum_{i=0}^{2^n-1} r_i |i\rangle = \underbrace{I \otimes \dots \otimes I}_{l+1} \otimes \underbrace{\sigma \otimes \dots \otimes \sigma}_{n-l-1} \sum_{i=0}^{2^n-1} b_i |i\rangle.$$

Then, from (D15), (D16) and (D17)

$$\begin{aligned} \sum_{i=0}^{2^{n-l}-1} p_{k*2^{n-l}+i} |i\rangle &= |0\rangle \otimes \sum_{i=0}^{2^{n-l-1}-1} (\tau_1 r_{k*2^{n-l}+i} + \tau_2 r_{k*2^{n-l}+2^{n-l-1}+i}) |i\rangle_{n-l-1} \\ &+ |1\rangle \otimes \sum_{i=0}^{2^{n-l-1}-1} (\tau_3 r_{k*2^{n-l}+i} + \tau_4 r_{k*2^{n-l}+2^{n-l-1}+i}) |i\rangle_{n-l-1}. \end{aligned} \quad (\text{D18})$$

Thus, from (D18)

$$p_{k*2^{n-l}+i} = \tau_1 r_{k*2^{n-l}+i} + \tau_2 r_{k*2^{n-l}+2^{n-l-1}+i}, p_{k*2^{n-l}+2^{n-l-1}+i} = \tau_3 r_{k*2^{n-l}+i} + \tau_4 r_{k*2^{n-l}+2^{n-l-1}+i}, \quad (\text{D19})$$

where $0 \leq k \leq 2^l - 1$ and $0 \leq i \leq 2^{n-l-1} - 1$.

By using the idea used in Step 2.1 above, from (D19) we can show $IV(p, n) = IV(r, n) \det(\tau)$.

Conclusively, it is not hard to prove Step 2 by repeating applications of Step 2.2.

Part 2. The proof of Theorem 2 (for odd n -qubits)

For the proofs for 3-qubits and 5-qubits, see Appendixes B and C, respectively.

The proof of Theorem 2 follows the following Steps 1 and 2 immediately.

Step 1. Prove

$$(\overline{IV}(a, n))^2 - 4IV^*(a, n-1)IV_{+2^{n-1}}^*(a, n-1) = (\overline{IV}(d, n))^2 - 4IV^*(d, n-1)IV_{+2^{n-1}}^*(d, n-1) \det(\alpha),$$

where $\overline{IV}(d, n)$, $IV^*(d, n-1)$ and $IV_{+2^{n-1}}^*(d, n-1)$ are obtained from $\overline{IV}(a, n)$, $IV^*(a, n-1)$ and $IV_{+2^{n-1}}^*(a, n-1)$ by replacing a by d , respectively.

Step 1.1. Prove

$$IV^*(a, n-1) = IV^*(d, n-1)\alpha_1^2 + \overline{IV}(d, n)\alpha_1\alpha_2 + IV_{+2^{n-1}}^*(d, n-1)\alpha_2^2.$$

By the definition,

$$IV^*(a, n-1) = \sum_{i=0}^{2^{n-3}-1} \text{sign}^*(n-1, i)(a_{2i}a_{(2^{n-1}-1)-2i} - a_{2i+1}a_{(2^{n-1}-2)-2i}).$$

When $0 \leq i \leq 2^{n-3} - 1$, clearly

$$0 \leq 2i, 2i+1, (2^{n-1}-2)-2i, (2^{n-1}-1)-2i \leq (2^{n-1}-1).$$

Hence, from (D1),

$$\begin{aligned} a_{2i} &= \alpha_1 d_{2i} + \alpha_2 d_{2^{n-1}+2i}, & a_{(2^{n-1}-1)-2i} &= \alpha_1 d_{(2^{n-1}-1)-2i} + \alpha_2 d_{2^{n-1}-2i}, \\ a_{2i+1} &= \alpha_1 d_{2i+1} + \alpha_2 d_{2^{n-1}+2i+1}, & a_{(2^{n-1}-2)-2i} &= \alpha_1 d_{(2^{n-1}-2)-2i} + \alpha_2 d_{2^{n-1}-2-2i}. \end{aligned} \quad (\text{D20})$$

By substituting (D20) into $IV^*(a, n-1)$,

$$\begin{aligned}
& IV^*(a, n-1) = \\
& \alpha_1^2 \sum_{i=0}^{2^{n-3}-1} \text{sign}^*(n-1, i)(d_{2i}d_{(2^{n-1}-1)-2i} - d_{2i+1}d_{(2^{n-1}-2)-2i}) \\
& + \alpha_1\alpha_2 \sum_{i=0}^{2^{n-3}-1} \text{sign}^*(n-1, i)[(d_{2i}d_{(2^n-1)-2i} - d_{2i+1}d_{(2^n-2)-2i}) - (d_{(2^{n-1}-2)-2i}d_{(2^{n-1}+1)+2i} - d_{(2^{n-1}-1)-2i}d_{2^{n-1}+2i})] \\
& + \alpha_2^2 \sum_{i=0}^{2^{n-3}-1} \text{sign}^*(n-1, i)(d_{2^{n-1}+2i}d_{(2^n-1)-2i} - d_{2^{n-1}+2i+1}d_{(2^n-2)-2i}) \\
= & IV^*(d, n-1)\alpha_1^2 + \overline{IV}(d, n)\alpha_1\alpha_2 + IV_{+2^{n-1}}^*(d, n-1)\alpha_2^2. \tag{D21}
\end{aligned}$$

Step 1.2. Calculating $IV_{+2^{n-1}}^*(a, n-1)$

As discussed in Step 1.1, we can demonstrate

$$IV_{+2^{n-1}}^*(a, n-1) = IV^*(d, n-1)\alpha_3^2 + \overline{IV}(d, n)\alpha_3\alpha_4 + IV_{+2^{n-1}}^*(d, n-1)\alpha_4^2.$$

Step 1.3. Prove

$$\overline{IV}(a, n) = 2 * IV^*(d, n-1)\alpha_1\alpha_3 + \overline{IV}(d, n)(\alpha_1\alpha_4 + \alpha_2\alpha_3) + 2 * IV_{+2^{n-1}}^*(d, n-1)\alpha_2\alpha_4.$$

By the definition,

$$\overline{IV}(a, n) = \sum_{i=0}^{2^{n-3}-1} \text{sign}(n, i)[(a_{2i}a_{(2^n-1)-2i} - a_{2i+1}a_{(2^n-2)-2i}) - (a_{(2^{n-1}-2)-2i}a_{(2^{n-1}+1)+2i} - a_{(2^{n-1}-1)-2i}a_{2^{n-1}+2i})].$$

When $0 \leq i \leq 2^{n-3}-1$, clearly

$$2^{n-1}-1 < (2^n-1)-2i, (2^n-2)-2i, (2^{n-1}+1)+2i, 2^{n-1}+2i.$$

Therefore, by (D1)

$$\begin{aligned}
a_{(2^n-1)-2i} &= \alpha_3 d_{(2^{n-1}-1)-2i} + \alpha_4 d_{2^{n-1}-2i}, a_{(2^n-2)-2i} = \alpha_3 d_{(2^{n-1}-2)-2i} + \alpha_4 d_{2^{n-2}-2i}, \\
a_{(2^{n-1}+1)+2i} &= \alpha_3 d_{2i+1} + \alpha_4 d_{2^{n-1}+1+2i}, a_{2^{n-1}+2i} = \alpha_3 d_{2i} + \alpha_4 d_{2^{n-1}+2i}. \tag{D22}
\end{aligned}$$

By substituting (D20) and (D22) and computing,

$$\begin{aligned}
& (a_{2i}a_{(2^n-1)-2i} - a_{2i+1}a_{(2^n-2)-2i}) - (a_{(2^{n-1}-2)-2i}a_{(2^{n-1}+1)+2i} - a_{(2^{n-1}-1)-2i}a_{2^{n-1}+2i}) = \\
& 2(d_{2i}d_{(2^{n-1}-1)-2i} - d_{2i+1}d_{(2^{n-1}-2)-2i})\alpha_1\alpha_3 \\
& + [(d_{2i}d_{(2^n-1)-2i} - d_{2i+1}d_{(2^n-2)-2i}) - (d_{(2^{n-1}-2)-2i}d_{2^{n-1}+2i+1} - d_{(2^{n-1}-1)-2i}d_{2^{n-1}+2i})](\alpha_1\alpha_4 + \alpha_2\alpha_3) \\
& + 2(d_{2^{n-1}+2i}d_{(2^n-1)-2i} - d_{2^{n-1}+2i+1}d_{(2^n-2)-2i})\alpha_2\alpha_4.
\end{aligned}$$

Note that when $0 \leq i \leq 2^{n-3}-1$, $\text{sign}^*(n, i) = \text{sign}(n, i)$ by the definition and $\text{sign}(n, i) = \text{sign}^*(n-1, i)$ by lemma 2. Thus, the proof of Step 1.3 is done.

By Steps 1.1, 1.2 and 1.3, we finish the proof of Step 1.

Step 2. Prove that

$$\begin{aligned}
& (\overline{IV}(d, n))^2 - 4IV^*(d, n-1)IV_{+2^{n-1}}^*(d, n-1) = \\
& [(\overline{IV}(b, n))^2 - 4IV^*(b, n-1)IV_{+2^{n-1}}^*(b, n-1)] \underbrace{\det(\beta)^2 \det(\gamma) \dots}_{n-1}.
\end{aligned}$$

By Theorem 1 for $(n-1)$ -qubits, from (D2),

$$IV^*(d, n-1) = IV^*(b, n-1) \underbrace{\det(\beta) \det(\gamma) \dots}_{n-1} \quad (\text{D23})$$

and from (D3)

$$IV_{+2^{n-1}}^*(d, n-1) = IV_{+2^{n-1}}^*(b, n-1) \underbrace{\det(\beta) \det(\gamma) \dots}_{n-1}. \quad (\text{D24})$$

Let us compute $\overline{IV}(d, n)$. From (D2) and (D3) we obtain

$$\sum_{i=0}^{2^{n-1}} (d_i - d_{2^{n-1}+i}) |i\rangle = \underbrace{\beta \otimes \gamma \dots}_{n-1} \sum_{i=0}^{2^{n-1}} (b_i - b_{2^{n-1}+i}) |i\rangle. \quad (\text{D25})$$

Let $d_i^* = d_i - d_{2^{n-1}+i}$ and $b_i^* = b_i - b_{2^{n-1}+i}$. Then (D25) can be rewritten as

$$\sum_{i=0}^{2^{n-1}} d_i^* |i\rangle = \underbrace{\beta \otimes \gamma \dots}_{n-1} \sum_{i=0}^{2^{n-1}} b_i^* |i\rangle. \quad (\text{D26})$$

By Theorem 1 for $(n-1)$ -qubits, from (D26) it is easy to see

$$IV^*(d^*, n-1) = IV^*(b^*, n-1) \underbrace{\det(\beta) \det(\gamma) \dots}_{n-1}. \quad (\text{D27})$$

Note that

$$IV^*(d^*, n-1) = \sum_{i=0}^{2^{n-3}-1} \text{sign}^*(n-1, i) (d_{2i}^* d_{(2^{n-1}-1)-2i}^* - d_{2i+1}^* d_{(2^{n-1}-2)-2i}^*)$$

and $\text{sign}^*(n-1, i) = \text{sign}(n, i)$ whenever $0 \leq i \leq 2^{n-3}-1$ by (??).

By expanding,

$$IV^*(d^*, n-1) = IV^*(d, n-1) + IV_{+2^{n-1}}^*(d, n-1) - \overline{IV}(d, n). \quad (\text{D28})$$

Similarly, by expanding,

$$IV(b^*, n-1) = IV^*(b, n-1) + IV_{+2^{n-1}}^*(b, n-1) - \overline{IV}(b, n). \quad (\text{D29})$$

Thus, substituting (D28) and (D29) into (D27), we have

$$\begin{aligned} IV^*(d, n-1) + IV_{+2^{n-1}}^*(d, n-1) - \overline{IV}(d, n) = \\ [IV^*(b, n-1) + IV_{+2^{n-1}}^*(b, n-1) - \overline{IV}(b, n)] \underbrace{\det(\beta) \det(\gamma) \dots}_{n-1}. \end{aligned} \quad (\text{D30})$$

From (D23), (D24) and (D30), we get

$$\overline{IV}(d, n) = \overline{IV}(b, n) \underbrace{\det(\beta) \det(\gamma) \dots}_{n-1}. \quad (\text{D31})$$

The proof of Step 2 follows (D23), (D24) and (D31) immediately.

Appendix E: The proof of $\tau \leq 1$

Let $f = (\overline{IV}(a, n))^2 - 4IV^*(a, n-1)IV_{+2^{n-1}}^*(a, n-1)$ and a_i be real. To find the extremes of f , we compute the following partial derivatives:

$$\text{from } \partial f / \partial a_0 = 0, \overline{IV}(a, n) \text{sign}(n, 0) a_{2^{n-1}} = 2IV_{+2^{n-1}}^*(a, n-1) \text{sign}^*(n-1, 0) a_{2^{n-1}-1}; \quad (\text{E1})$$

$$\text{from } \partial f / \partial a_1 = 0, \overline{IV}(a, n) \text{sign}(n, 0) a_{2^{n-2}} = 2IV_{+2^{n-1}}^*(a, n-1) \text{sign}^*(n-1, 0) a_{2^{n-1}-2}; \quad (\text{E2})$$

.....

$$\text{from } \partial f / \partial a_{2^{n-1}-2} = 0, \overline{IV}(a, n) \text{sign}(n, 0) a_{2^{n-1}+1} = 2IV_{+2^{n-1}}^*(a, n-1) \text{sign}^*(n-1, 0) a_1; \quad (\text{E3})$$

$$\text{from } \partial f / \partial a_{2^{n-1}-1} = 0, \overline{IV}(a, n) \text{sign}(n, 0) a_{2^{n-1}} = 2IV_{+2^{n-1}}^*(a, n-1) \text{sign}^*(n-1, 0) a_0; \quad (\text{E4})$$

$$\text{from } \partial f / \partial a_{2^{n-1}} = 0, \overline{IV}(a, n) \text{sign}(n, 0) a_{2^{n-1}-1} = 2IV^*(a, n-1) \text{sign}^*(n-1, 0) a_{2^{n-1}}; \quad (\text{E5})$$

.....

$$\text{from } \partial f / \partial a_{2^{n-1}} = 0, \overline{IV}(a, n) \text{sign}(n, 0) a_0 = 2IV^*(a, n-1) \text{sign}^*(n-1, 0) a_{2^{n-1}}. \quad (\text{E6})$$

From (E1) \times (E4),

$$(\overline{IV}(a, n))^2 \text{sign}(n, 0) a_{2^{n-1}} a_{2^{n-1}} = 4(IV_{+2^{n-1}}^*(a, n-1))^2 \text{sign}^*(n-1, 0) a_0 a_{2^{n-1}-1}. \quad (\text{E7})$$

From (E2) \times (E3),

$$(\overline{IV}(a, n))^2 \text{sign}(n, 0) a_{2^{n-1}+1} a_{2^{n-2}} = 4(IV_{+2^{n-1}}^*(a, n-1))^2 \text{sign}^*(n-1, 0) a_1 a_{2^{n-1}-2}. \quad (\text{E8})$$

.....

From (E7)–(E8),

$$\begin{aligned} & (\overline{IV}(a, n))^2 \text{sign}(n, 0) (a_{2^{n-1}} a_{2^{n-1}} - a_{2^{n-1}+1} a_{2^{n-2}}) = \\ & 4(IV_{+2^{n-1}}^*(a, n-1))^2 \text{sign}^*(n-1, 0) (a_0 a_{2^{n-1}-1} - a_1 a_{2^{n-1}-2}). \end{aligned} \quad (\text{E9})$$

.....

Evaluate the sum over the above expressions like (E9), we obtain

$$(\overline{IV}(a, n))^2 IV_{+2^{n-1}}^*(a, n-1) = 4(IV_{+2^{n-1}}^*(a, n-1))^2 IV^*(a, n-1). \quad (\text{E10})$$

As well, we have

$$(\overline{IV}(a, n))^2 IV^*(a, n-1) = 4(IV^*(a, n-1))^2 IV_{+2^{n-1}}^*(a, n-1). \quad (\text{E11})$$

From (E10), $IV_{+2^{n-1}}^*(a, n-1) = 0$ or $f = 0$. From (E11), $IV^*(a, n-1) = 0$ or $f = 0$. When $IV_{+2^{n-1}}^*(a, n-1) = 0$ or $IV^*(a, n-1) = 0$, it is not hard to see that $f = (\overline{IV}(a, n))^2 \leq 1/4$. When $f = 1/4$, $|a_j| = |a_{2^{n-1}-j}|$.

Therefore $0 \leq f \leq 1/4$ and $0 \leq \tau \leq 1$.

References

- [1] C. H. Bennett et al, quant-ph/9908073.
- [2] C. H. Bennett et al, Phys. Rev. A 63, 0123072001.
- [3] A. Aćin et al., quant-ph/0003050.
- [4] W. Dür, G.Vidal and J.I. Cirac, Phys. Rev. A. 62 (2000)062314.

- [5] A. Acin, E. Jane, W.Dür and G.vidal, Phys. Rev. Lett. 85, 4811 (2000).
- [6] H.J.Briegel and R.Raussendorf, Phy. Rev. Lett. 86, 910 (2001).
- [7] H.K.LO and S. Popescu, Phys. Rev. A. 63 02230 (2001).
- [8] F. Verstraete, J.Dehaene and B.De Moor, Phys. Rev. A. 65, 032308 (2002).
- [9] F. Verstraete, J.Dehaene, B.De Moor and H. Verschelde Phys. Rev. A. 65, 052112 (2002).
- [10] A. Miyake, PRA 67, 012108 (2003).
- [11] A.Miyake, quant-ph/0401023.
- [12] A.K. Rajagopal and R.W. Rendell, PRA 65, 032328 (2002).
- [13] D. Li et al., Simple criteria for the SLOCC classification, Phys. Lett. A 359, 428(2006).
- [14] D. Li et al., submitted to JPA, quant-ph/070132.
- [15] D. Li et al., the necessary and sufficient conditions for separability for multipartite pure states, unpublished, submitted to PRL, the paper No. LV9637(Sep. 2004) and quant-ph/0604147.
- [16] V. Coffman et al., PRA 61, 052306 (2000).
- [17] Chang-shui Yu and He-shan Song, PRA 71, 042331(2005).
- [18] A. Wong and N. Christensen, PRA 63, 044301(2001).
- [19] A. Osterloh and J. Siewert, PRA 72, 012337(2005).
- [20] A. Osterloh and J. Siewert, International journal of quantum information Vol. 4, No.3 (2006) 531-540.